Source Document: Government of Canada Federated Architecture Iteration One June 2000

Link to entire Document : http://www.cio-dpi.gc.ca/fap-paf/documents/iteration/iteration09_e.asp

Architecture Principles

Architecture principles are a crucial foundation for a federated architecture. They have a "timeless" quality because they define a value system (while methodologies frequently change, as a rule, values do not). Architecture principles are stable. Once they are established, only very slight adjustments are needed to address changing business strategies and priorities. If significant modifications are required, their impact is rigorously assessed through a formal change management process.

Each principle consists of four parts: a short name, brief description, rationale for the principle (typically in business terms for the technical principle), and implications or consequences (positive and negative) of adopting the principle.

The following architecture principles were derived from the specific requirements in the Common Requirements Vision. They are primarily concerned with guiding the development of information systems and technology infrastructure in support of Government On-Line (GOL), Tier 1.

Architecture Principle 1: Reduce Integration Complexity

The federated architecture must promote reduced complexity and enable integration to the maximum extent possible. We must re-engineer application systems to be "highly modular" and "loosely coupled" to be able to reuse components.

Rationale:

- complex application systems that have many data and transactional functions are difficult to manage and change is risky;
- applications that have tightly coupled or linked modules risk creating a dependency failure;
- to adapt to multiple geographic requirements from users (i.e. users in many different locations) and take advantage of distributed processing powers, applications must be deployed on multiple physical servers;
- reusable components must be deployed independently of the deployment platform.; and
- commercial components are or will be available for many business functions.

Implications:

Reducing integration complexity means:

- component-based and compatible application development;
- keeping to a minimum the number of vendors, products and configurations, allowing for maximum flexibility in implementing changes;

- minimising configurations of architectural components and discouraging custom tuning, or “customisation” of hardware and software based on transient local or other conditions;
- maintaining “configuration discipline,” sacrificing performance and functionality in some instances;
- an increasing reliance on “infrastructure subassemblies” supplied by vendors;
- more, smaller application or infrastructure components or modules;
- less change;
- fundamental to component-based design of applications and infrastructure;
- less redundancy between applications and infrastructure components;
- establishing a “culture of reuse” through the use of incentives;
- building and integrating reusable components must become a common development method;
- making component management a core competency;
- making design and analysis for business logic systemic to the application environment. In other words, applications need to be designed so that the components that are used to define the business logic are reused when there are available and only created if a component of business logic does not exist;
- shared systems and systems components; and
- establishing physical configuration standards.

Architecture Principle 2: Holistic Approach

Information is a government asset. Its value is enhanced when it can be accessed and applied to accelerate decision making, which is leveraged through interdepartmental collaboration within the bounds of legislation and privacy. The infrastructure must promote a “whole of government” approach while respecting unique federal government roles and mandates.

Rationale:

- the value of information is not always realised when it remains in isolated pockets;
- information must be shared to maximise the effectiveness of business decision making throughout the government and beyond to external partners;
- decision making needs to accelerate to support shrinking business process cycle times;
- more effective decision making requires increasing the integrity and relevance of data;
- a government-wide approach to infrastructure is the best way to leverage IT capital investments by eliminating duplicate infrastructure and support services, and leveraging economies of scale where appropriate; and

- as government business processes continue to change, it will be easier and quicker to adapt the IT infrastructure to facilitate this change if it is designed with a “whole of government” approach.

Implications:

A holistic approach means:

- identifying and exploiting the information “value chain”;
- unifying data/information management;
- restructuring data for easy access and management;
- identifying and specifying authoritative sources;
- promoting an understanding of “infostructure” throughout government;
- establishing data warehouses to facilitate information availability for decision making;
- accelerating information “velocity” and establishing a policy for information sharing;
- programs and services providing corporate access to specified data/information;
- developing a standardised mechanism for evaluating technical alternatives;
- establishing rules and decision criteria to distinguish when unique departmental requirements related to common infrastructure take precedence over the government-wide approach;
- emphasising solutions that can apply government-wide;
- organising business systems and databases according to subject matter, not department, division or unit;
- accepting that decisions could take longer to make, and solutions could require more time to implement; and
- departments and organisations occasionally conceding their own preferences for the greater benefit of the entire federal government.

Architecture Principle 3: Business Event-Driven Systems

Systems must be designed to be business event-driven. This principle applies to manual, process and application systems. Further, application systems must keep the operational data necessary to allow the government to re-create any business event.

Rationale:

- enables the infrastructure to support enhancing the adaptability of the government’s business processes because business process change involves adding, removing or modifying business events;
- strengthens the linkage between the infrastructure and the business process;
- systems are being designed to conform to actual events, rather than the system dictating the required user interfaces;

- it is easier to realign business processes when change occurs; and
- from the legal and liability perspective, supports data retention which is of paramount importance.

Implications:

Business Event-Driven Systems means:

- replacing batch logic with event-driven logic;
- replacing batch processing with asynchronous processing;
- more systemic thinking as event-based processing generally crosses traditional system boundaries;
- shifting to a “push” model of information delivery;
- retaining data for extended periods of time and making it accessible to operational systems; and
- ensuring disaster recovery and business resumption planning takes critical data and systems into consideration.

Architecture Principle 4: Defined Authoritative Sources

All information must have defined “authoritative sources.” These sources will act as information stewards. Authorized data must be accessible and available for re-use by any entitled systems and/or business process.

Rationale:

- data needs to be made available in a timely and accurate form and therefore must be captured and validated once, at the source;
- information needs to be useful, usable and reliable to be of value to the government and its citizens; and
- supporting event-driven systems means that information must be validated at source.

Implications:

Defined authoritative sources means:

- assigning departments accountability for data that is captured within their application systems;
- making data owners accountable for the definition and quality of the data;
- establishing government-wide procedures to manage data access and ensure data security and integrity; and
- applying fully defined data verification rules to transactions in real time.

Architecture Principle 5: Security, Confidentiality, Privacy and Protection of Information

IT systems must be implemented in adherence with government security, confidentiality and privacy policies and laws. Information must be protected against unauthorized access, denial of service, and both intentional and accidental modification.

Rationale:

- helps safeguard client information;
- enhances public trust;
- protects government assets;
- enables compliance with public funding requirements;
- minimises improper use of data, which can have serious business and legal consequences; and
- minimises a security violation, which impair integrity and jeopardise the government's viability.

Implications:

Security, confidentiality, privacy and protection of information means:

- identifying, publishing and keeping the applicable IM policies current;
- monitoring compliance;
- making the security, confidentiality and privacy requirements clear to designers, developers, etc;
- implementing approaches/policies to minimise improper use of data;
- implementing approaches/policies to minimise security violations; and
- clearly articulated policy for use of information.

Architecture Principle 6: Proven Standards and Technologies

IT solutions must use commercially viable standards-based technologies. The customization of purchased software must be avoided wherever possible. Priority will be given to products adhering to industry standards and open architecture. Where multiple standards apply, the following order of precedence shall prevail:

i. Government of Canada approved and interim standards, and technical reports (e.g. CSE Common Criteria);
ii. National Standards of Canada and CSA standards;
iii. International (i.e. ISO) Standards and ITU recommendations;
iv. Other publicly-developed standards including IETF and industry consortia specifications; and
v. De facto standards.

Rational:

- avoids dependence on weak and/or under performing vendors;
- reduces risk;
- ensures robust product support;
- enables greater use of standard, shareable components and Commercial Off the Shelf (COTS) solutions;
- allows government to influence and stay current with industry standards and trends;
- purchased packages can be selected for “functionality” fit with business requirements and speed of delivery; and
- allows flexibility and adaptability in product replacement.

Implications:

Provende technologies means :

- establishing criteria to identify weak or under performing vendors and standard products;
- moving away from weak products in the current application portfolio;
- assessing the architectural fit of the package;
- potentially modifying work practices and business workflow to increase standards compliance;
- vendors making changes to purchased software and maintaining them in their base product; and
- making a culture shift towards setting and monitoring standards and compliance.

Architecture Principle 7: Total Cost of Ownership (TCO)

Total Cost of Ownership for applications and technologies (hardware and software) must balance development, support, disaster recovery and retirement costs along with the costs of flexibility, scalability, ease of use/support over the life cycle of the technology or application.

Rationale:

- leads to higher quality solutions;
- reduces Total Cost of Ownership;
- enables improved planning and budget decision making; and
- Total Cost of Ownership includes the design, construction, and operation and maintenance for government-wide integrated systems.

Implications:
Total Cost of Ownership means:

- designers and developers must take a systemic view;
- pursuing sub-optimisation on a selective basis in order to ensure that the overall system is optimised;
- developing a way to identify Total Cost of Ownership; and
- increasing information sharing related to Total Cost of Ownership of projects.

Architecture Principle 8: Plan for Growth
IT must plan, design, and construct for growth and expansion of services (known requirements) across government.

Rationale:
- more cost-effective;
- recognises that hardware is cheaper than labour;
- reduces maintenance costs; and
- enables quicker response to growth and change.

Implications:
Planning for growth means:

- making a culture shift in adaptive thinking;
- developing ways to predict growth from historical trends; and
- capacity planning.

Architecture Principle 9: Adopt Formal Methods of Engineering
Government must employ formal practices, methods, and tools for architecture and engineering for all stages of these disciplines in IM/IT, from design to implementation and construction.

Rationale:
- reduces training costs;
- reduces reliance on project management and staff;
- leads to benchmarks for measurement;
- enables improved quality assurance; and
- enables repeatability and consistency.

Implications:
Adopting formal methods of engineering means:

- agreeing on practices and methods;
- developing a process definition function;
- developing practice and method training; and
- monitoring for compliance.

Architecture Principle 10: Extended Information and Services Environment
To the extent possible, the integration of the IM/IT infrastructure must enable the provision of Government of Canada information and services to citizens, businesses, and other governments (i.e. provincial, municipal and international).

Rationale:
A number of the services that citizens and business expect from government require co-ordination with partners and other levels of government. To respond efficiently and provide the expected level of service, certain partners and other levels of government must be incorporated within a government information and services environment. An extended trusted government information environment also broadens the potential channels through which clients can access information and services.

Implications:
Developing an extended information and services environment means:

- identifying the Government of Canada programs to be optimised;
- identifying partners;
- developing terms and conditions for the sharing of information and services;
- determining what information and services need to be shared;
- reviewing existing policy and legislation; and
- analysing the current environment to target and prioritise what must be done.

Architecture Principle 11: Multiple Delivery Channels
Support client delivery channel preferences in accessing government services.

Rationale:
- citizens, businesses and partners want channels of service delivery from the federal government that suit their individual preferences and circumstances; and
- depending on the nature of the program being delivered, the circumstances of the transaction and the sensitivity of the information involved, specific services lend themselves to specific

channels; and multiple delivery channels also protect against having a single point failure and help ensure that vital services can still be delivered.

Implications:

Maintaining multiple channels of service delivery means:

- products and services may be accessed in a variety of ways, but must be available to users in an integrated, consistent fashion;
- there should be a common, look and feel, common standards for privacy and security and consistent service quality regardless of choice of delivery channel;
- clients can access a number of delivery channels simultaneously, particularly in the event of an ESD failure; and
- applications must be designed to be delivery channel independent.

Architecture Principle 12: Accessible Government

To be responsive to the increasing diversity of Canadian society, the Government of Canada must be accessible to all citizens.

Rationale:

The federal government has a responsibility to ensure that it can provide services to all citizens. Therefore, it must be accessible to all citizens and address their specific access requirements.

Implications:

Accessible government means:

- presenting and configuring information to make it easier for citizens to interact with government and obtain information;
- making the ways that information is displayed and accessed adaptable to meet a wide range of citizens' needs and access preferences;
- ensuring that guidelines for citizen interfaces are not constrained by narrow assumptions about location, language, systems training or physical and cognitive capabilities;.
- adopting a wide range of principles to promote accessibility; and
- pursuing "universal design" which in the context of technology refers to the design of products, systems, processes and environments. This means components are usable by all people to the greatest extent possible, without the need for system-wide adaptation and yet with the capability to receive technical customisation (retrofitting) on an individualised basis.

The following are sub-principles related to universal design to be applied in the architecture and included in the IM/IT infrastructure by Core and Domain architecture teams:

- Equitable Use: Accommodating *all* users in relation to electronic networks. This means that delivery of services must occur simultaneously for all accessibility needs.

- Flexibility of Use: While promoting a degree of standardisation and compatibility with various electronic information technologies, accommodating a wide range of individual preferences and abilities.

- Simple and Intuitive Use: Ensuring ease of comprehension and use, regardless of the user's experience, knowledge, language skills, or concentration level.

- Perceptible Information: Communicating information effectively, regardless of the user's physical and/or sensory abilities, so that it can be used efficiently and comfortably with a minimum of fatigue.

Architecture Principle 13: Robustness

Implemented infrastructure must be robust, responsive, and reliable with appropriate redundancy to protect against system failure.

Rationale:

- The federal government provides many essential services that especially in times of crisis must be available upon demand and in a compressed time frame.

- To maintain expected business service levels, it will be necessary to sub-optimise certain parts of the infrastructure, by selecting more stable technologies that provide fewer features.

- It will also be necessary to suboptimize the Total Cost of Ownership to ensure desired business service levels are attained.

Implications:

Robustness means:

- The infrastructure design must take into consideration likely points of failure and providing backup and redundant components.

implication